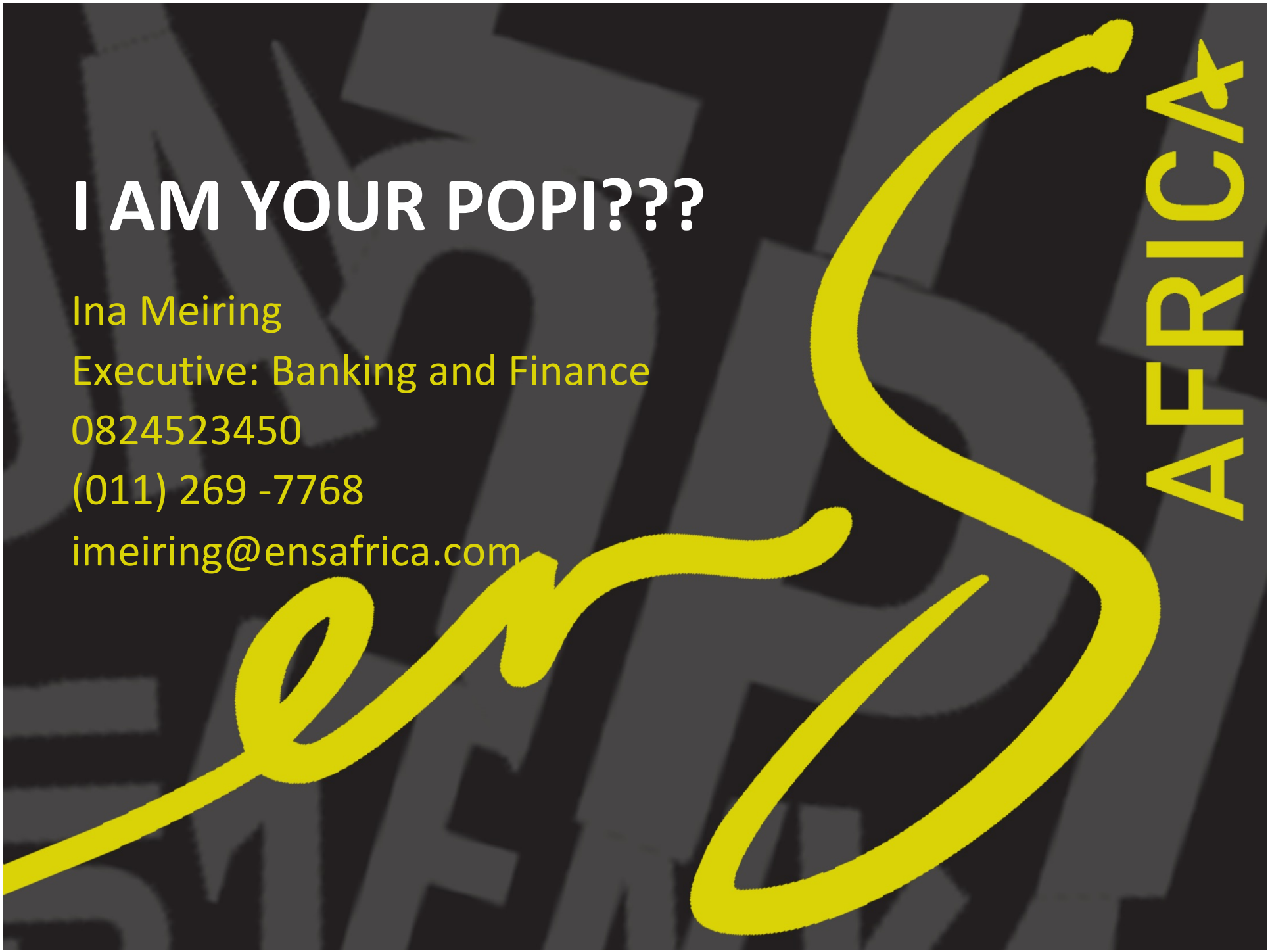
I AM YOUR POPI???

Ina Meiring
Executive: Banking and Finance
0824523450
(011) 269 -7768
imeiring@ensafrica.com



POPI timeline & milestones

20 Aug 2013
National Assembly passed the Protection of Personal Information Bill [B9D of 2009]

19 Nov 2013
Signed into law by the President

Section 115 - Act will come into force on a date to be determined by the President by proclamation in the Gazette

24 Jul 2015
Parliament calls for nominations for candidates for five positions within the Regulator

8 Sep 2017
Publish draft regulations for public comment

7 Nov 2017 Closing date for public comments

Transitional period of 1 year

11 Apr 2014
Regulations, Regulator and definitions

13 Apr 2016
The Portfolio Committee on Justice and Correctional Services ("the Committee") shortlists 10 candidates for positions within the Regulator

17 May 2016
Committee recommends Adv. **Pansy Tlakula** be appointed as chairperson and four other candidates as members of the Regulator

1 Dec 2016
Regulator appointed

INFORMATION REGULATOR (SOUTH AFRICA)

Feb – Mar 2018
Submission for tabling of the draft regulations to Parliament

2018
Anticipated date of Publication of final Regulations in Government Gazette

Regulations

- 17 Forms: Examples -
- Objection to the processing of personal information
- Request for correction or deletion of personal information
- Application for the issue of a code of conduct
- Consent for direct marketing

Information Officer must ensure that -

- a compliance framework is developed, implemented and monitored;
- adequate measures and standards exists in order to comply with the conditions for the lawful processing of personal information;
- preliminary assessments are conducted;
- internal measures are developed together with adequate systems to process requests for information or access thereto;
- awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.

Manual

- The Information Officer must ensure that a manual for the purpose of the Promotion of Access to Information Act and the Act is developed detailing—
- (i) the purpose of the processing;
- (ii) a description of the categories of data subjects and of the information or categories of information relating thereto;
- (iii) the recipients or categories of recipients to whom the personal information may be supplied;
- (iv) the planned trans-border or cross border flows of personal information; and
- (v) a general description allowing preliminary assessment of the suitability of information security measures to be implemented and monitored by the responsible party;

Manual

- The manual must be available—
- (i) on the website, of the responsible party; and
- (ii) at the office or offices of the responsible party for public inspection during normal business hours of that responsible party.

Direct marketing

- Direct marketing by means of unsolicited electronic communications.
- Section 69: (1) The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject-
- has given his, her or its consent to the processing; or
- is a customer of the responsible party.

Direct marketing

- A responsible party may approach a data subject whose consent is required, and who has not previously withheld such consent, only once in order to request the consent of that data subject.
- A responsible party may request a data subject's consent in writing on a form which corresponds substantially with Form 4 to the Annexure for the processing of personal information of that data subject for the purpose of direct marketing as contemplated in section 69(2) of the Act.

Cross-border transfers

- A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless-
- the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that-
- (i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

Cross-border transfers (continued)

- (ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

Cross-border transfers (continued)

- the transfer is for the benefit of the data subject, and-
- (i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and
- (ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

Interpretation

- Section 3(3)(a) of POPI provides that the Act must be interpreted in a manner that gives effect to the purpose of POPI set out in section 2.
- Section 2(b) provides that one of the purposes of POPI is to regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards that prescribe the minimum threshold requirements for the lawful processing of personal information.
- EU's General Data Protection Regulation ("**GDPR**")

Application of the GDPR

- The EU's General Data Protection Regulation ("GDPR") became effective on 25 May 2018.
- Extra-territorial application
- Article 3(2) of the GDPR provides that it applies to the processing of personal data of data subjects who are in the EU by a controller or processor (i.e. the responsible party and operator) not established in the EU, where the processing activities are related to:
  - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
  - the monitoring of their behaviour as far as their behaviour takes place within the EU.

Legitimate interest

- Guidance given by the UK Information Commissioner's Office ("**ICO**") re the expectations around using legitimate interest as a basis for processing personal information. Three-part test:
- Purpose test – is there a legitimate interest behind the processing?
- Necessity test – is the processing necessary for that purpose?
- Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms?
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

Legitimate interest

- The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list.
- It also says that you have a legitimate interest in disclosing information about possible criminal acts or security threats to the authorities.

Legitimate interest

- First, identify the legitimate interest(s). Consider:
- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Legitimate interests

- Second, apply the necessity test. Consider:
- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Legitimate interests

- Third, do a balancing test. Questions may include -
- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are any of the individuals vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?

Questions